Section III.2. Ideals

Note. Ideals are to rings as normal subgroups are to groups. We will use ideals to define quotient rings. We'll state isomorphism theorems, define direct products, and prove the Chinese Remainder Theorem.

Definition III.2.1. Let R be a ring and S a nonempty subset of R that is closed under the operations of addition and multiplication in R. If S is itself a ring under these operations then S is a *subring* of R. A subring I of R is a *left ideal* provided

$$r \in R \text{ and } x \in I \text{ implies } rx \in I;$$

I is a *right ideal* provided

$$r \in R \text{ and } x \in I \text{ implies } xr \in I;$$

I is an *ideal* if it is both a left and right ideal.

Note. If $f : R \to S$ is a homomorphism of rings then (as we'll see in Theorem III.2.8 and as we'd expect given our approach to quotient groups) $\text{Ker}(f)$ is an ideal in R and $\text{Im}(f)$ is a subring of S. For each $n \in \mathbb{Z}$, $\langle n \rangle$ is an ideal in $\mathbb{Z}$. For any ring R, two ideals are the trivial ideal $\{0\}$ and the improper ideal R.

Note. Let D be a division ring and R the ring of $n \times n$ matrices over D. Let I_k be the set of all matrices that have zero entries except possibly in column k. Then I_k is a left ideal (but not a right ideal) of R (because of the row $\times$ column product

of matrices). Let J_k consists of those matrices with zero entries except possibly in row k. Then J_k is a right ideal of R (but not a left ideal). Ring R has no "proper" two sided ideals, however (see Exercise III.2.9).

Note III.2.A. As with subgroups, we call ideal I *proper* in R if $I \neq \{0\}$ and $I \neq R$. Notice that if R has identity (or "unity") 1_R and if 1_R is in ideal I then $I = R$. In fact, if u is a unit in R and $u \in I$, then $1_R = uu^{-1} \in I$ and so $I = R$. If $1_R \notin I$ then $I \neq R$. So we can say that a left (or right) nonzero ideal I of ring R with identity 1_R is proper if and only if I contains no units of R. So a division ring (in which every nonzero element is a unit) has no proper left (or right) ideals.

Theorem III.2.2. A nonempty subset I of a ring R is a left (respectively, right) ideal if and only if for all $a, b \in I$ and $r \in R$:

(i) $a, b \in I$ implies $a - b \in I$, and

(ii) $a \in I$, $r \in R$ implies $ra \in I$ (respectively, $ar \in I$).

Note. The following is a very straightforward implication of Theorem II.2.2.

Corollary III.2.3. Let $\{A_i \mid i \in I\}$ be a family of left (respectively, right) ideals in a ring R. Then $\cap_{i \in I} A_i$ is also a left (respectively, right) ideal of R.

Definition III.2.4. Let X be a subset of a ring R. Let $\{A_i \mid i \in I\}$ be the family of all left (respectively, right) ideals in R which contains X. Then $\cap_{i\in I} A_i$ is the left (respectively, right) *ideal generated by* X, denoted (X). The elements of X are *generators* of (X). If $|X|$ is finite then (X) is *finitely generated*. An ideal generated by a single element x, denoted (x), is a *principal ideal*. A *principal ideal ring* is a ring in which every ideal is principal. A principal ideal ring which is an integral domain is a *principal ideal domain* (or "PID").

Theorem III.2.5. Let R be a ring $a \in R$ and $X \subset R$.

(i) The principal ideal (a) consists of all elements of the form

$$ra + as + na + \sum_{i=1}^{m} r_i a s_i$$

where $r, s, r_i, s_i \in R$, $m \in \mathbb{N} \cup \{0\}$, and $n \in \mathbb{Z}$.

(ii) If R has an identity ("unity") then

$$(a) = \left\{ \sum_{i=1}^{n} r_i a s_i \mid r_i, s_i \in R, n \in \mathbb{N} \right\}.$$

(iii) If a is in the center of R, $C(R) = \{c \in R \mid cr = rc \text{ for all } r \in R\}$, then $(a) = \{ra + na \mid r \in R, n \in \mathbb{Z}\}$.

(iv) $Ra = \{ra \mid r \in R\}$ (respectively, $aR = \{ar \mid r \in R\}$), is a left (respectively, right) ideal in R (which may not contain a). If R has an identity, then $a \in Ra$ and $a \in aR$.

(v) If R has an identity and a is in the center of R, then $Ra = (a) = aR$.

(vi) If R has an identity and X is the center of R, then the ideal (X) consists of all finite sums $r_1a_1 + r_2a_2 + \cdots + r_na_n$ where $n \in \mathbb{N} \cup \{0\}$, $r_i \in R$, and $a_i \in X$.

Definition. Let $A_1, A_2, \ldots, A_n$ be nonempty subsets of ring R. Define

$$A_1 + A_2 + \cdots + A_n = \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i \text{ for } i = 1, 2, \ldots, n\}.$$

If AB are nonempty subsets of R define

$$AB = \{a_1b_1 + a_2b_2 + \cdots + a_nb_n \mid a_i \in A_i, b_i \in B_i, n \in \mathbb{N}\}.$$

If $A_1, A_2, \ldots, A_n$ are nonempty, define

$$A_1A_2 \cdots A_n = \{a_1^1a_2^1 \cdots a_n^1 + a_1^2a_2^2 \cdots a_n^2 + \cdots + a_1^ma_2^m \cdots a_n^m \mid a_i^j \in A_i, m \in \mathbb{N}\}.$$

We denote $\{a\}B = aB$, $A\{b\} = Ab$, and $AA \cdots A = A^n$.

Theorem III.2.6. Let $A_1, A_2, \ldots, A_n, B, C$ be left (respectively, right) ideals in a ring R.

(i) $A_1 + A_2 + \cdots + A_n$ and $A_1A_2 \cdots A_n$ are left (respectively, right) ideals.

(ii) $(A + B) + C = A + (B + C)$.

(iii) $(AB)C = ABC = A(BC)$.

(iv) $B(A_1 + A_2 + \cdots + A_n) = BA_1 + BA_2 + \cdots + BA_n$ and $(A_1 + A_2 + \cdots + A_n)C = A_1C + A_2C + \cdots A_nC$.

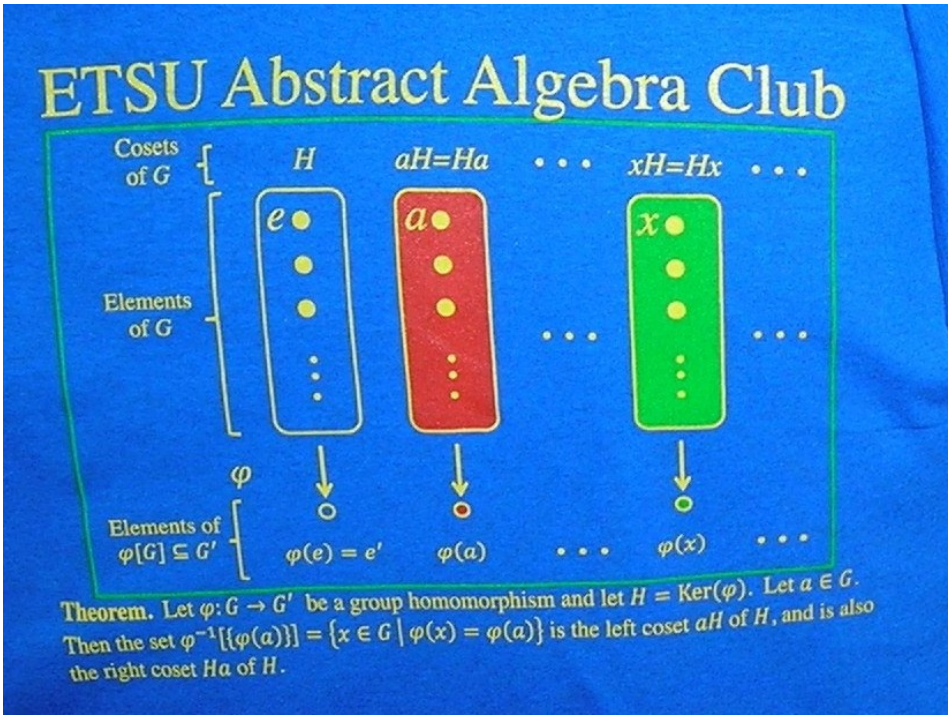
Note III.2.B. For R a ring, $\langle R, + \rangle$ is an abelian group and an ideal I of R determines a normal subgroup $\langle I, + \rangle$ of $\langle R, + \rangle$. So the quotient group R/I exists. In fact, the cosets in R/I can be multiplied in the obvious way (by representatives) and so R/I has a ring structure.

Theorem III.2.7. Let R be a ring and I an ideal of R. Then the additive quotient group R/I is a ring with multiplication given by

$$(a+I)(b+I) = ab+I.$$

If R is commutative or has an identity, then the same is true of R/I.

Note. The following result is analogous to Theorem I.5.5. You might recall that Fraleigh initially sets up quotient groups using kernels of homomorphisms. See my online notes for Introduction to Modern Algebra (MATH 4127/5127) on Section III.13. Homomorphisms and Section 14. Factor Groups. Also, check out the front of the ETSU Abstract Algebra Club t-shirt:



Theorem III.2.8. If $f : R \to S$ is a homomorphism of rings then the kernel of f is an ideal in R. Conversely if I is an ideal in R then the map $\pi : R \to R/I$ given by $r \mapsto r + I$ is an onto homomorphism (epimorphism) of rings with kernel I.

Note. We now present several results for "quotient rings" which are parallel to results from Section I.5 for quotient groups.

Theorem III.2.9. If $f : R \to S$ is a homomorphism of rings and I is an ideal of R which is contained in the kernel of f, then there is a unique homomorphism of rings $\overline{f} : R/I \to S$ such that $\overline{f}(a + I) = f(a)$ for all $a \in R$. $\text{Im}(\overline{f}) = \text{Im}(f)$ and $\text{Ker}(\overline{f}) = \text{Ker}(f)/I$. $\overline{f}$ is an isomorphism if and only if f is an epimorphism and $I = \text{Ker}(f)$.

Corollary III.2.10. First Isomorphism Theorem.
If $f : R \to S$ is a homomorphism of rings, then f induces an isomorphism of rings $R/\text{Ker}(f) \cong \text{Im}(f)$.

Corollary III.2.11. If $f : R \to S$ is a homomorphism of rings, I is an ideal in R, and J is an ideal in S such that $f(I) \subset J$, then f induces a homomorphism of rings $\overline{f} : R/I \to S/J$, given by $a + I \mapsto f(s) + J$. $\overline{f}$ is an isomorphism if and only if $\text{Im}(f) + J = S$ and $f^{-1}(J) \subset I$. In particular, if f is an epimorphism such that $f(I) = J$ and $\text{Ker}(f) \subset I$, then $\overline{F}$ is an isomorphism.

Theorem III.2.12. Let I and J be ideals in a ring R.

(i) Second Isomorphism Theorem.

There is an isomorphism of rings $I/(I \cap J) \cong (I + J)/J$.

(ii) Third Isomorphism Theorem.

If $I \subset J$, then J/I is an ideal in R/I and there is an isomorphism of rings $(R/I)/(J/I) \cong R/J$.

Note. The four previous results follow easily once we quote the corresponding result for quotient groups from Section I.5. Then we need only verify the homomorphism property for multiplication. The correspondences are:

Ring Result	**Group Result**
Theorem III.2.9	Theorem I.5.6
Corollary III.2.10	Corollary I.5.7
Corollary III.2.11	Corollary I.5.8
Theorem III.2.12(i)	Corollary I.5.9
Theorem III.2.12(ii)	Corollary I.5.10

Theorem III.2.13. If I is an ideal in a ring R, then there is a one-to-one correspondence (i.e., bijection) between the set of all ideals of R which contain I and the set of all ideals of R/I, given by $J \mapsto J/I$. Hence every ideal in R/I is of the form J/I where J is an ideal of R which contains I.

Definition III.2.14. An ideal P in a ring R is *prime* if $P \neq R$ and for any ideals A, B in R

$$AB \subset P \text{ implies } A \subset P \text{ or } B \subset P.$$

Note. Exercise III.2.14 gives some classification of prime ideals:

Exercise III.2.14. If P is an ideal in (not necessarily commutative) ring R, then the following conditions are equivalent:

(a) P is a prime ideal.

(b) If $r, s \in R$ are such that $rRs \subset P$, then $r \in P$ or $s \in P$.

(c) If (r) and (s) are principal ideals of R such that $(r)(s) \subset P$, then $r \in P$ or $s \in P$.

(d) If U and V are right ideals in R such that $UV \subset P$, then $U \subset P$ or $V \subset P$.

(e) If U and V are left ideals in R such that $UV \subset P$, then $U \subset P$ or $V \subset P$.

Note. The following result gives a classification of prime ideals in a *commutative* ring.

Theorem III.2.15. If P is an ideal in a ring R such that $P \neq R$ and for all $a, b \in R$

$$ab \in P \text{ implies } a \in P \text{ or } b \in P \qquad (1)$$

then P is prime. Conversely if P is prime and R is commutative, then P satisfies condition (1).

Note. Exercise III.2.9(b) shows (by a general example) that commutativity is necessary in the converse part of Theorem III.2.15.

Note. Another reason for the terminology "prime" ideal is inspired by considering the prime ideal (p) for prime integer p in ring $\mathbb{Z}$. Then

$$ab \in (p) \Longrightarrow p \mid ab \Longrightarrow p \mid a \text{ or } p \mid b \Longrightarrow a \in (p) \text{ or } b \in (p).$$

Theorem III.2.16. In a commutative ring R with identity $1_R \neq 0$, an ideal P is prime if and only if the quotient ring R/P is an integral domain.

Definition III.2.17. An ideal M in a ring R is said to be *maximal* if $M \neq R$ and for every ideal N such that $M \subset N \subset R$, either $N = M$ or $N = R$. A *maximal left* or *maximal right ideal* is similarly defined.

Theorem III.2.18. In a nonzero ring R with identity, maximal ideals always exist. In fact, every ideal in R (except R itself) is contained in a maximal ideal. This also holds for left ideals and right ideals.

Note. Theorem III.2.18 is further evidence for the desirability of accepting the Axiom of Choice and its logical equivalent, Zorn's Lemma. It guarantees the existence of maximal ideals.

Theorem III.2.19. If R is a commutative ring such that $RR = R^2 = R$ (in particular, if R has an identity) then every maximal ideal M in R is prime.

Theorem III.2.20. Let M be an ideal in a ring R with identity $1_R \neq 0$.

(i) If M is maximal and R is commutative then the quotient ring R/M is a field.

(ii) If the quotient ring R/M is a division ring, then M is maximal.

Note III.2.C. Since a field is an example of a division ring, Theorem III.2.20 implies that for M an ideal in ring R with identity $1_R \neq 0$, the quotient ring R/M is a filed if and only if M is a maximal ideal. As shown in Exercise III.2.19 with an example, Theorem III.2.20(i) is false if R does not have an (multiplicative) identity.

Note. The following result gives conditions equivalent to a commutative ring being a field.

Corollary III.2.21. The following conditions on a commutative ring R with identity $1_R \neq 0$ are equivalent.

(i) R is a field.

(ii) R has no proper ideals.

(iii) $\{0\}$ is a maximal ideal in R.

(iv) Every nonzero homomorphism of rings $R \to S$ is injective (a "monomorphism").

Note. The following result allows us to define the (external) direct product of a family of rings.

Theorem III.2.22. Let $\{R_i \mid i \in I\}$ be a nonempty family of rings and $\prod_{i\in I} R_i$ the direct product of additive abelian groups R_i.

(i) $\prod_{i\in I} R_i$ is a ring with multiplication defined by $\{a_i\}_{i\in I}\{b_i\}_{i\in I} = \{a_i b_i\}_{i\in I}$.

(ii) If R_i has an identity (respectively, is commutative) for every $i \in I$, then $\prod_{i\in I} R_i$ has an identity (respectively, is commutative).

(iii) For each $k \in I$ the canonical projection $\pi_k : \prod_{i\in I} R_i \to R_k$ given by $\{a_i\} \mapsto a_k$ is an epimorphism (onto) of rings.

(iv) For each $k \in I$ the canonical injection $\iota_k : R_k \to \prod_{i\in I} R_i$, given by $a_k \mapsto \{a_i\}$ (where $a_i = 0$ for $i \neq k$) is a monomorphism (one to one) of rings.

Definition. Let $\{R_i \mid i \in I\}$ be a family of rings. $\prod_{i\in I} R_i$ as given in Theorem III.2.22 is the (*external*) *direct product* of the family.

Note. If $\{R_i \mid i \in I\}$ is a family of rings and for each $i \in I$, A_i is an ideal in R_i, then "it is easy to see" (Hungerford, page 130) that $\prod_{i\in I} A_i$ is an ideal in $\prod_{i\in I} R_i$. If the index set I is finite and each R_i has an identity, then *every* ideal in $\prod_{i\in I} R_i$ is of the form $\prod_{i\in I} A_i$ with A_i an ideal in R_i (see Exercise III.2.22).

Theorem III.2.23. Let $\{R_i \mid i \in I\}$ be a nonempty family of rings S a ring and $\{\varphi_i : S \to R_i \mid i \in I\}$ a family of homomorphisms of rings. Then there is a unique homomorphism of rings $\varphi : S \to \prod_{i\in I} R_i$ such that $\pi_i\varphi = \varphi_i$ for all $i \in I$ where π_i is the canonical projection of Theorem III.2.22. The ring $\prod_{i\in I} R_i$ is uniquely determined up to isomorphism by this property. In other words $\prod_{i\in I} R_i$ is a product in the category of rings.

Theorem III.2.24. Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

(i) $A_1 + A_2 + \cdots + A_n = R$, and

(ii) for each k, with $1 \leq k \leq n$, $A_k \cap (A_1 + A_2 + \cdots + A_{k-1} + A_{k+1} + \cdots A_n) = \{0\}$.

Then there is a ring isomorphism $R \cong A_1 \times A_2 \times \cdots \times A_n$.

Definition. If $A_1, A_2, \ldots, A_n$ are ideals of ring R satisfying the hypotheses of Theorem III.2.24 then R is a (*internal*) *direct product* of the ideals A_i.

Note. There is a subtle distinction between internal and external direct products; one not-so-subtle difference is that an external direct product is defined over any family of rings, whereas an internal direct product is only defined over a finite collection of ideals in a ring (recall that ideals are themselves rings). If R "is" the internal direct product of ideals $A_1, A_2, \ldots, A_n$ then each A_i is an ideal contained in R but the A_i's are not contained in $A_1 \times A_2 \times \cdots \times A_n$, only isomorphic images of the A_i's are contained in the product (under the canonical injection of Theorem II.2.22(iv)).

Note. We now explore the Chinese Remainder Theorem which will be needed in Chapters VIII and IX when a detailed study of rings is continued (so we can skip the rest of this chapter if we are pushed for time).

Definition. Let A be an ideal in a ring R and $a, b \in R$. Then a and b are *congruent modulo* A (denoted $a \equiv b \pmod{A}$) if $a - b \in A$.

Theorem III.2.25. Chinese Remainder Theorem.
Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that $R^2 + A_i = R$ for all i and $A_i + A_j = R$ for all $i \neq j$. If $b_1, b_2, \ldots, b_n \in R$, then there exists $b \in R$ such that

$$b \equiv b_i \pmod{A_i} \text{ for } i = 1, 2, \ldots, n.$$

Furthermore, b is uniquely determined up to congruence modulo the ideal

$$A_1 \cap A_2 \cap \cdots \cap A_n.$$

Note. The Chinese Remainder Theorem is applicable to questions in elementary number theory as follows. Suppose we are looking for an integer x which is congruent to 3 modulo 5, 2 modulo 7, and 5 modulo 11. Since 5, 7, and 11 are relatively prime, then if we find one such integer x we can find others by considering those integers congruent to x modulo $5 \times 7 \times 11 = 385$. The Chinese Remainder Theorem does not say *how* to find x, but merely insures that such x exists. In this example, $x = 93$ (or any other integer equivalent to 93 modulo 385). The Chinese Remainder Theorem is explored in Introduction to Number Theory (MATH 3120); see my

online notes for that class on Section 5. Linear Congruences; see Theorem 5.2. You can find calculators online which find the smallest positive x; see for example David Wees' Chinese Remainder Theorem Calculator (accessed 1/21/2024).

Corollary III.2.26. Let $m_1, m_2, \ldots, m_n$ be positive integers such that $(m_i, m_j) = 1$ for $i \neq j$. If $b_1, b_2, \ldots, b_n$ are any integers, then the system of congruences

$$x \equiv b_1 (\text{mod } m_1),\ x \equiv b_2 (\text{mod } m_2), \ldots,\ x \equiv b_n (\text{mod } m_n)$$

has an integral solution that is uniquely determined modulo $m = m_1 m_2 \cdots m_n$.

Note. The earliest example of a question involving the ideas of Corollary III.2.26 appear in Sun Zi's *Sun Zi suanjing* ("*Master Sun's Mathematical Manual*"). Sun Zi is though to have lived from about 400 to 460. See the MacTutor webpage on the Chinese mathematics (accessed 1/21/2024). This is the reason the result is called the "Chinese Remainder Theorem," (though Hungerford's timeline of "the first century A.D." for the result is mysterious).

Corollary III.2.27. If $A_1, A_2, \ldots, A_n$ are ideals in a ring R, then there is a monomorphism of rings

$$\theta : R/(A_1 \cap A_2 \cap \cdots \cap A_n) \to R/A_1 \times R/A_2 \times \cdots \times R/A_n.$$

If $R^2 + A_i = R$ for all i and $A_i + A_j = R$ for all $i \neq j$, then θ is an isomorphism of rings.